EFT POLICY

2017/2018 FINANCIAL YEAR

Midvaal Local Municipality recognises that the use of electronic funds transfer as a faster, easier and more efficient method of payment to creditors.

Internal controls such as written policies and procedures, authorisations, segregation of duties and monitoring are still important in the new technological world.

Electronic banking will be used for, but not limited to, the following:

- Online banking services (reviewing account balances, retrieving bank statements
- Paying of creditors
- Paying of salaries
- Refund of billing payments
- Investment of funds in accordance with Council investment policy.

1. Municipal Expenditure

All expenditure of Midvaal Local Municipality shall be incurred in terms of section 11 of the MFMA. The accounting system has built-in controls which prevents duplicate payments of the same invoice.

2. Electronic Fund Transfer

The Chief Financial Officer shall delegate officials in writing for authority to process electronic payments. One person should not be allowed to process transactions from beginning to end single handedly. A minimum of four officials should be allowed to process EFT's on behalf of the municipality. This practice shall ensure the segregation of duties and division of authority in order to minimise fraud.

Delegation shall be made in terms of Section 79 of the MFMA.

Only the Accounting Officer or the Chief Financial Officer of Midvaal Local Municipality or any other delegated senior financial officer of the municipality acting on written authority of the Accounting Officer, may authorise the withdrawal of money from Midvaal Local Municipality's bank account through signature on a cheque or Electronic

Fund Transfer. Such withdrawals shall be accompanied by official expenditure documents which are duly authorised for purposes as prescribed in section 11(a)-(j) of the MFMA.

Officials delegated in terms of Section 79 of the MFMA:

- Assistant Director Expenditure
- Chief Financial Officer
- Deputy Chief Financial Officer
- Director Expenditure
- Assistant Director: Financial Control

Once an EFT transaction has been completed, the payment list with banking details, together with the supporting documentation, is submitted to the Deputy Chief Financial Officer for final verification.

3. Banking details

Suppliers banking details are captured onto the system once the completed bank stamped electronic funds transfer form which is received. Once captured, the bank details are then verified and authorised on the system. Banking details cannot be captured and authorised by the same official, thereby ensuring segregation of duties.

An audit trail of changes to bank details is printed and verified monthly.

4. Controls for EFT users

Access to the banking system is restricted to authorised officials. These officials are authorised by completing a request for user form which is then signed by the authorised signatories at the bank.

The bank manager would then send a bank official to verify the user and grant him/her access to the system from their PC. Users have a login name and are required to have two passwords. The user is prompted by the system on a monthly basis to change the second password. The first password can be voluntarily changed whenever the user wants to. If you have logged on and have not used the service for three minutes, you will be logged off. To access your account, you will need to LOGON again. You have three opportunities to enter your password correctly. After the third unsuccessful attempt, you will be denied access to the service. You will then be required to call the Helpdesk to have the password reset.

A user is temporarily suspended from using the system if they have not accessed the system for more than a month. Once suspended, the user will have to contact the bank to re-instate their access. Two different users are required to effect an EFT transaction, as two approvals are required before a payment is made. Both approvals have to be made the same day, otherwise the transaction is aborted.

5. Additional Precautions

The following precautions should be taken when entering user codes and passwords on the internet:

- Check to make sure that the URL begins with "https" rather than "http".
- Ensure that the website has a security certificate
- Always ensure the secrecy of your password